Process Safety Beacon
Messages for Manufacturing Personnel
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

This issue sponsored by
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Cyber Security και Χημικές Λειτουργίες

Ιούλιος 2021

Εικόνα 1. Oldmar, Florida εγκατάσταση επεξεργασίας νερού

Στις 5 Φεβρουαρίου 2021, ένας εργαζόμενος στην εγκατάσταση επεξεργασίας νερού στο Oldsmar, Florida, παρατήρησε ότι ο κέρσορας κινούταν περίεργα στην οθόνη του υπολογιστή του. Αρχικά, δεν υπήρχε καμία ανησυχία· η εγκατάσταση χρησιμοποιούσε λογισμικό απομακρυσμένης πρόσβασης για να επιτρέπει στο προσωπικό το διαμοιρασμό της οθόνης και να επιλύει θέματα IT. Ο προϊστάμενος συχνά συνδεόταν στον υπολογιστή του χειριστή για να παρακολουθεί επίσης τα συστήματα της εγκατάστασης. Μερικές ώρες αργότερα, ο χειριστής παρατήρησε ότι ο κέρσορας κινούταν και επέλεγε τα συστήματα ελέγχου της εγκατάστασης επεξεργασίας νερού. Μέσα σε δευτερόλεπτα, ο εισβολέας προσπαθούσε να αλλάξει το σημείο αναφοράς του υδροξειδίου του νατρίου από 100 μέρη στο εκατομμύριο (ppm) σε 11.100 ppm. Ο χειριστής εντόπισε γρήγορα της εισβολή και επανέφερε το υδροξείδιο του νατρίου σε κανονικά επίπεδα. Ευτυχώς, δεν υπήρξε καμία επίπτωση στην ποιότητα του νερού.

Μια πρόσφατη επίθεση με λογισμικό εκβίασης (ransomware) στην εταιρία Colonial Pipeline διέκοψε την εφοδιασμό βενζίνης στην Ανατολική Ακτή των ΗΠΑ για αρκετές μέρες.

Τα συστήματα της εταιρίας σας είναι πιθανότατα συνδεδεμένα στο Διαδίκτυο και χρειάζονται προστασία από τις κυβερνοαπειλές. Υπάρχουν πολλές στρατηγικές που χρησιμοποιούνται από εταιρίες για την αποτροπή κυβερνοαπειλών, όπως: τείχη προστασίας, λογισμικό προστασίας από ιούς και πολιτικές για την προστασία από κακόβουλα προγράμματα και ιούς υπολογιστών.

Όλο και περισσότερα άτομα εργάζονται εξ αποστάσεως· αυτό έχει αυξήσει τις ευκαιρίες για κυβερνοεπιθέσεις.

Το γνωρίζατε;

- Οι κυβερνοεγκληματίες χρησιμοποιούν εξελιγμένο κακόβουλο λογισμικό για να επωφεληθούν από πολλαπλά τρωτά σημεία και να πετύχουν τους στόχους τους.
- Οι επιθέσεις με λογισμικό εκβίασης αυξάνονται με τους οργανωμένους ‘εγκληματίες’ να το χρησιμοποιούν σαν εργαλείο αποκόμισης κερδών.
- Σύμφωνα με μια πρόσφατη μελέτη, κάθε 39 δευτερόλεπτα συμβαίνει μια κυβερνοεπίθεση. (Πηγή: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Το ηλεκτρονικό «ψάρεμα» συμβαίνει όταν υποτιθέμενες αξιόπιστες εταιρίες, στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου, με σκοπό να ωθήσουν άτομα να αποκαλύψουν προσωπικές πληροφορίες.
- Οι κυβερνοαπειλές μπορούν να εισέλθουν στα συστήματα της εταιρείας μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, συνημμένων αρχείων και από φορητές συσκευές αποθήκευσης, όπως ‘φλασάκια’ ή άλλες παρόμοιες συσκευές.
- Το ενενήντα πέντε τοις εκατό των παραβιάσεων της κυβερνοασφάλειας προκαλείται από ανθρώπινο λάθος. (Πηγή: https://www.cybintsolutions.com/employee-education-reduces-risk/)

Τί μπορούμε να κάνουμε;

- Πάντα να επαληθεύουμε τα αιτήματα ενημέρωσης λογισμικού με το IT πριν συνεχίσουμε και να εγκαθιστούμε εγκαίρως τις εγκεκριμένες ενημερώσεις.
- Να βεβαιωνόμαστε ότι τα τείχη προστασίας και άλλα λογισμικά δικτύου είναι ενημερωμένα και ενεργοποιημένα.
- Να φροντίζουμε να δημιουργούμε τακτικά αντίγραφα ασφαλείας των συστημάτων και των δεδομένων μας.
- Να χρησιμοποιούμε ισχυρούς προσωπικούς κωδικούς για όλες τις προσβάσεις. Να μην μοιραζόμαστε τους κωδικούς πρόσβασης ή τους λογαριασμούς και να αλλάζουμε τακτικά τους κωδικούς πρόσβασης.
- Να μην αποθηκεύουμε κωδικούς πρόσβασης σε προγράμματα περιήγησης.
- Να μην επιλέγουμε συνδέσμους ή συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται από κάποιον που δεν γνωρίζουμε.
- Να μην εγκαθιστάμε ποτέ μη εγκεκριμένο λογισμικό σε οποιονδήποτε εταιρικό υπολογιστή· να βεβαιωνόμαστε ότι οι κωδικοί πρόσβασης και άλλες συσκευές φυσικής ασφάλειας είναι σωστά προστατευμένες.
- Αν χρησιμοποιούμε την απομακρυσμένη πρόσβαση, να ακολουθούμε τις απαιτήσεις της εταιρείας. Να είμαστε ιδιαίτερα προσεκτικοί αν χρησιμοποιούμε δημόσιους ιστότοπους στο διαδίκτυο.
- Αν κάτι στον υπολογιστή μας φαίνεται περίεργο ή διαφορετικό, να ζητήσουμε βοήθεια! Μπορεί να είναι ένας κακόβουλος χρήστης (hacker) που προσπαθεί να αποκτήσει πρόσβαση.

Οι κυεβερνοεπιθέσεις είναι πραγματικές. Είμαστε ζωτικό μέρος της άμυνας.

©AIChE 2021. All rights reserved. Reproduction for non-commercial, educational purposes is encouraged. However, reproduction for any commercial purpose without express written consent of AIChE is strictly prohibited. Contact us at ccps_beacon@aiche.org or 646-495-1371.